UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

IN RE: TARGET CORPORATION CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates to: All Financial Institution and Consumer Cases	MDL No. 14-2522 (PAM/JJK)

FINANCIAL INSTITUTION AND CONSUMER PLAINTIFFS' JOINT MEMORANDUM IN OPPOSITION TO TARGET CORPORATION'S MOTION TO STAY DISCOVERY

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE

Cases:

PAGE

PAGE

PAGE

I. PRELIMINARY STATEMENT

Fact discovery should begin and should not be delayed. As set forth below, federal courts disfavor staying discovery while a motion to dismiss is pending, and here, Target[1] has not met ***its burden*** of demonstrating that its anticipated motion to dismiss will resolve all claims in its favor.

In fact, a review of other data-breach cases and the undisputed facts here suggest that Plaintiffs' claims are virtually certain to overcome a motion to dismiss in some form. Moreover, Target's requested stay would prejudice Plaintiffs by further delaying the prosecution of their claims, which were first filed in December 2013, and seriously jeopardize the July 1, 2015 discovery cut-off deadline established by the Court. (*See* ECF Nos. 93, 94.) Finally, Target's arguments that Financial Institution Plaintiffs' claims will be dismissed and that Consumer Plaintiffs lack standing are premature and incorrect. Neither argument warrants a stay of discovery. Accordingly, this Court should deny Target's Motion.

II. RELEVANT FACTUAL BACKGROUND

Target failed to properly secure its computer systems and safeguard customers' account data, resulting in a massive data security breach of approximately 110 million Target customer credit and debit card information in 2013 and harming consumers nationwide and causing significant monetary losses to consumers and financial

[1] References to "Target," "Defendants," or the "Company" collectively refer to defendants Target Corporation, Target Brands, Inc., Target Corporate Services, Inc. and Target.com.

institutions. Plaintiffs' case descriptions set forth in their May 7, 2014 Case Management Conference Briefs are incorporated here. (ECF Nos. 31, 34.) Additional background information to assist the Court in considering Target's motion follows.

Congressional hearings followed the security breach in February 2014, and Target's security measures are being investigated by the Department of Justice, the U.S. Secret Service, the Federal Trade Commission, and several state law enforcement agencies. Target officials testified before Congress that the company only began investigating on December 12, 2013 when the Department of Justice warned the company about suspicious activity involving payment cards. According to a New York Times report, the attackers first gained access to Target's internal network on November 12, 2013. Elizabeth A. Harris, et al., *A Sneaky Path Into Target Customers' Wallets*, N.Y. Times (Jan. 17, 2014), http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html.

According to a report issued March 26, 2014, by the Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883 ("Senate Committee Report"), the hackers who breached Target's system have sold, and continue to sell, the stolen information via black market internet forums known as "card shops." Criminals purchase this stolen information and use it to make new, phony cards that can be used to make fraudulent purchases. The Senate Committee Report's analysis "suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the

massive data breach." *Id.* Key points at which Target apparently failed to detect and stop the attack include, but are not limited to, the following:

- Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network.

- Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.

- Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.

- Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.

Id. The Senate Committee Report further states:

> According to a *Bloomberg Businessweek* report, Target's FireEye malware intrusion detection system triggered urgent alerts with each installation of the data exfiltration malware. However, Target's security team neither reacted to the alarms nor allowed the FireEye software to automatically delete the malware in question.

Id. at 3.[2] The Senate Committee Report explains that "[t]he attackers transmitted the stolen data to outside servers – at least one of which was located in Russia" and goes on to state:

---

[2] The *Bloomberg Businessweek* report referenced in the Senate Committee Report states:

> In testimony before Congress, Target has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened. What it hasn't publicly revealed: Poring over computer logs,

> Target's FireEye software reportedly did detect the data exfiltration malware and decoded the destination of servers on which data for millions of stolen credit cards were stored for days at a time. Acting on this information could have stopped the exfiltration, not only at this last stage, but especially during the "delivery" step on the kill chain.

Id. at 11.

Plaintiffs contend that Target, among other things, (1) failed to take reasonable measures to protect their financial and personal information, allowing cyber thieves to exploit vulnerabilities in Target's point-of-sale systems and to access and extract customer data for resale on the black market; (2) failed to comply with industry data-protection standards; (3) caused Consumer Plaintiffs monetary losses, by allowing the data thieves to, for example, place unauthorized charges on counterfeit cards, open new lines of credit, and drain bank accounts; (4) exposed Consumer Plaintiffs to a continuing, certainly impending risk of additional misuse, fraud, and identity theft; (5) caused massive injury to Financial Institution Plaintiffs, estimated eventually to be billions of dollars in costs associated with, among other things, cancelling and reissuing credit and

---

> Target found FireEye's alerts from Nov. 30 and more from Dec. 2, when hackers installed yet another version of the malware. Not only should those alarms have been impossible to miss, they went off early enough that the hackers hadn't begun transmitting the stolen card data out of Target's network. Had the company's security team responded when it was supposed to, the theft that has since engulfed Target, touched as many as one in three American consumers, and led to an international manhunt for the hackers never would have happened at al.

Michael Riley, et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It, Bloomberg Businessweek* (Mar. 13, 2014), http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

debit cards, monitoring and stopping payments with respect to fraud-related charges, refunding fraudulent charges, closing and re-opening checking and savings accounts affected by the breach, and notifying their customers of the breach; and (6) failed to disclose material facts concerning the inadequacy of its security systems such that had Consumer Plaintiffs known of Target's substandard security procedures and methods of collecting and storing customers' personal information, they would have paid substantially less for Target's goods and services, or would have not shopped at Target's retail stores at all (*i.e.*, Plaintiffs would have purchased the same product from a different in-store consumer-goods retailer).

III. ARGUMENT

A. Courts disfavor staying discovery.

Pursuant to Fed. R. Civ. P. 26(c), a court may stay discovery only upon "good cause" shown to protect a party from annoyance, embarrassment, oppression, undue burden or undue expense. "[T]he determination is practical, and largely left to the district court's discretion." *TE Connectivity Networks, Inc. v. All Sys. Broadband, Inc.*, Civ. No. 13-1356 ADM/FLN, 2013 WL 4487505, at *2 (D. Minn. Aug. 20, 2013) (denying motion to stay where responding to discovery would not be "unusually burdensome or prejudicial" and where "it does not appear the Complaint is facially frivolous or clearly without merit"); *see also Baer v. G&T Trucking Co.*, No. 03-cv-3460, slip op. ECF No. 30 at 2 (D. Minn. Feb. 23, 2004) (Magnuson, J.) (denying defendant's motion to stay discovery in a putative class action) (Decl. of Jeffrey D. Bores (Bores Decl.) Ex. A).

Nothing in the Federal Rules provides that discovery should be stayed pending a motion to dismiss, and if it did, it would "require the court to make a preliminary finding of the likelihood of success on the motion to dismiss," circumventing the procedures for resolution of such a motion. *Gray v. First Winthrop Corp.*, 133 F.R.D. 39, 40 (N.D. Cal. 1990) (denying stay in securities class action pending motion to dismiss). Indeed, courts recognize that "[m]otions to stay discovery are not favored because when discovery is delayed or prolonged it can create case management problems which impede the court's responsibility to expedite discovery and cause unnecessary litigation expenses and problems." *Castro v. Sanofi Pasteur, Inc.*, No. 2:11-cv-07178, Order at 2, (D.N.J. July 18, 2012) (ECF No. 102) (quotation omitted) (Bores Decl. Ex. B). It is "black letter law that the mere filing of a motion to dismiss the complaint does not constitute 'good cause' for the issuance of a discovery stay." *TE Connectivity Networks, Inc.*, 2013 WL 4487505, at *2 (citation omitted); *accord Hachette Distrib., Inc. v. Hudson Cnty. News Co.*, 136 F.R.D. 356, 359 (E.D.N.Y. 1991); *Gerald Chamales Corp. v. Oki Data Ams., Inc.*, 247 F.R.D. 453, 454 (D.N.J. 2007). As previously noted by Judge Montgomery:

> [A]lthough [defendant] has filed a potentially viable motion to dismiss, it has not demonstrated any specific good cause warranting a stay. This case does not involve a statute or doctrine of law which requires the resolution of motions to dismiss before discovery begins. Nor has [defendant] indicated any particular facts or circumstances that make responding to discovery in this case unusually burdensome or prejudicial beyond the usual case of this nature. Without good cause based in either law or fact, the motion to stay will be denied.

TE Connectivity Networks, Inc., 2013 WL 4487505, at *2. Indeed, Target's arguments seeking a stay of all discovery (e.g, claims may be narrowed) are generic ones applicable

to any case where a motion to dismiss will be filed. *See In re Plastics Additives Antitrust Litig.*, No. Civ. 03-2038, 2004 WL 2743591, at *7 (E.D. Pa. Nov. 29, 2004) (denying motion to stay discovery and noting that "although the defendants may experience some future prejudice if this Court refuses to grant a stay of merits-based discovery . . . this prejudice is both remote and uncertain"). Target's arguments fall well short of the standard needed for the extraordinary relief it seeks. *See TE Connectivity Networks, Inc.*, 2013 WL 4487505, at *2.

B. Financial Institution Plaintiffs' claims will survive Target's Motion to Dismiss.

Financial Institution Plaintiffs have incurred significant damages from Target's data security breach.[3] Target's bald assertion that it cannot be held liable for these damages under any theory of recovery because of arguments it intends to raise in a motion to dismiss, is simply wrong and does not meet the standard for staying all discovery. (Defs.' Mem. in Support of Motion to Stay Discovery ("Defs.' Mem.") at 11 (ECF No. 126).) Financial Institution Plaintiffs' Consolidated Complaint will be filed on August 1, 2014, and, amply supported by applicable law, will assert claims based in tort and contract and pursuant to Minnesota statute. While premature to raise hypothetical arguments against the sufficiency of a yet-to-be-filed complaint, as previewed below, taking a "peek" at Financial Institution Plaintiffs' claims establish that these claims are well-founded and supported both in law and in fact. *See id*. Moreover, rather than support Target's arguments in favor of a discovery stay, other data breach cases cited by

[3] *See e.g., First Farmers & Merchants Nat'l Bank, et al v. Target Corp.*, No. 14-cv-497, ECF No. 1 at ¶¶7-8 (D. Minn. filed Feb. 22, 2014).

Target (*In re Heartland*, *In re TJX Cos. Retail Security Breach Litig.*, and *Sovereign Bank v. BJ's Wholesale Club, Inc.* (*see* Defs.' Mem. at 12, n.12, 14-17)), actually support ***denial*** of Target's motion. Although those courts took different positions on the breach of contract and tort claims under their respective states' laws, the plaintiffs' actions proceeded to discovery in all instances. Thus, certain core facts relevant across all claims will be discovered. Accordingly, there is no basis for granting the extraordinary relief Target seeks.

1. Target is liable to the Financial Institution Plaintiffs under a negligence theory.

Financial Institution Plaintiffs have asserted straightforward negligence claims. Yet Target suggests that the Court will be required to make a "groundbreaking duty ruling" (*see* Defs.' Mem. at 13) for these claims to proceed. That is simply not the case. Target owed a duty to exercise reasonable care to Financial Institution Plaintiffs to whom injury was foreseeable. *Gaudreault v. Elite Line Servs., LLC*, No. 12-cv-1177, 2014 WL 2117211, at *5 (D. Minn. May 21, 2014). This Court need not create a special test to assess the sufficiency of Financial Institution Plaintiffs' negligence claims. *Compare id. with* Defs.' Mem. at 11.

The harm suffered by Financial Institution Plaintiffs as a result of Target's failure to exercise reasonable care to safeguard financial data, including, *inter alia*, the cost to cancel and reissue affected cards and to reimburse consumers for fraudulent transactions, was eminently foreseeable by Target. Courts applying the foreseeability standard in other data breach cases have found that financial institutions are foreseeable victims of a

merchant's data breach. *See In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, MDL No. 2046, 2011 WL 1232352, at *23 (S.D. Tex. Mar. 31, 2011) (finding financial institutions are foreseeable victims of data breach because they are "identifiable, and the kinds of damages alleged—stemming primarily from card replacement and charging off fraudulent transactions—are straightforward");[4] *see also Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 426 (5th Cir. 2013) ("***Heartland had reason to foresee the Issuer Banks would be the entities to suffer economic losses were Heartland negligent***" (emphasis added)). There is nothing "groundbreaking" about holding negligent parties responsible for harm they inflicted upon foreseeable victims. *See Lone Star Nat'l Bank*, 729 F.3d at 426 (refusing to dismiss issuer banks' negligence claim against defendant); *see also Gaudreault*, 2014 WL 2117211, at *5 (holding plaintiff "made a sufficient showing" that defendants' motion for summary judgment regarding plaintiffs' negligence claim "must be denied").

Target's authorities do not alter this result or warrant a discovery stay. *See, e.g., Castro*, Order at 2; *see also Baer*, slip op. at 2. For example, Target cites to *Erickson v. Curtis Inv. Co.*, 447 N.W.2d 165 (Minn. 1989), and *Funchess v. Cecil Newman Corp.*, 632 N.W.2d 666 (Minn. 2001) to argue that Minnesota law would be "reluctant" to impose a duty to protect business entities. (Defs.' Mem. at 13.) Both cases are

[4] The *Heartland* district court's dismissal of negligence claims under New Jersey's economic loss rule was subsequently reversed by the Fifth Circuit Court of Appeals. *See Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 426 (5th Cir. 2013); *see also* Defs.' Mem. at 13, n.13 (citing *Lone Star Nat'l Bank*). Target does not argue that the economic loss doctrine is applicable to Financial Institution Plaintiffs' claims in this case.

inapposite. First, *Erickson* involved the claims of a parking ramp customer who was attacked by a third party and later filed suit against the owner and operator of the ramp and the security firm that had been hired to patrol the premises. 447 N.W.2d at 168. Second, *Erickson* actually ***rejected*** arguments that the defendant owed the plaintiff no duty, concluding instead that there were fact issues. *Id.* at 166, 169-70 (concluding on appeal from summary judgment after full discovery that "[t]he operator or owner of a parking ramp facility ***has a duty*** to use reasonable care to deter criminal activity on its premises which may cause personal harm to customers.") (emphasis added)). "Whether a duty is imposed depends on the . . . relationship of the parties and the foreseeable risk involved." *Id.* at 168-69.

Target is not a blameless defendant being pursued by wholly unforeseeable victims. Rather, Target knowingly failed to prevent the breach from occurring, and then failed to respond to the breach by processing thousands of transactions at the Financial Institution Plaintiffs' expense once the breach occurred. Target maintained ineffective data protection safeguards and inexplicably ignored multiple red flags while the data breach was occurring under its nose. Had Target acted as a reasonably prudent corporation under the circumstances by maintaining a properly secured data collection system and immediately alerting Financial Institutional Plaintiffs of the breach, Financial Institution Plaintiffs could have limited their losses. The law does not immunize Target's negligence. *See Heartland*, 2011 WL 1232352, at *23 (financial institutions are foreseeable victims). In addition, the Minnesota legislature has explicitly recognized financial institutions as foreseeable victims of data breach events. *See* Minn. Stat. §

325E.64, subd. 3 (titled the "Minnesota Plastic Card Security Act" and allowing "financial institutions" to recover "costs of reasonable actions" undertaken in response to a data breach).

Funchess does not help Target either. (Defs.' Mem. at 13.) In that case – rendered at the summary judgment stage – heirs of a tenant murdered in his apartment by third party intruders brought a wrongful death action against the landlord, alleging that the landlord's negligence in failing to repair a security door lock and intercom in the tenant's building contributed to the tenant's death. 632 N.W.2d at 668. The Minnesota Supreme Court concluded that the landlord was not under a duty to protect the tenant from the criminal attack ***under the specific facts of that case***. *See id.* at 675 ("Although there may be other circumstances in which the duty to maintain security measures would give rise to liability for injuries of the type presented here, those circumstances do not exist in this case."). The Supreme Court, however, did not provide blanket immunity to businesses for all third party acts under all circumstances. *See id.* Moreover, other data breach cases have expressly held that "the criminal acts of the third parties ***did not*** break the chain of causation." *Id.* (emphasis added); *see Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp. 2d 183, 196 (M.D. Pa. 2005) ("[defendants'] lack-of-causation argument should be rejected"); *see also* Minn. Stat. § 325E.64, subd. 3.[5]

[5] Defendants' other cited cases (*see* Defs.' Mem. at 11-12) do not warrant staying all discovery. First, *Digital Federal Credit Union v. Hannaford Brothers*, No. BCD-CV-10-4, 2012 WL 1521479 (Me. B.C.D. Mar. 14, 2012) found that no duty existed under Maine law based on enactments ***by Maine's legislature***. *See id.* at *3. Accordingly, *Digital Federal Credit Union* has limited relevance.

Not only does Target cite distinguishable case law, they ignore authority clearly supporting the Financial Institution Plaintiffs' negligence claims. For example, in *Sovereign Bank*, 395 F. Supp. 2d 183, a merchant moved to dismiss an issuing bank's claims after thieves stole bank-card information from the merchant, arguing no duty. *See id.* at 194. The court held that the bank sufficiently alleged a duty owed by the merchant to the issuing bank. *Id.* at 193-95[6] (merchant and bank had a "sufficient relationship").

Target also ignores *Heartland*, where the court recognized a merchant's duty in very similar circumstances. 2011 WL 1232352 *Id.* at *22 (citing *People Express Airlines, Inc. v. Consol. Rail Corp.*, 495 A.2d 107, 116 (N.J. 1985)). The *Heartland* court held that the financial institution plaintiffs there had satisfied the foreseeability test at the pleading stage, reasoning that "the financial institutions participating ***are*** identifiable, and

---

Second, the court in *BancFirst v. Dixie Restaurants, Inc.*, No. 11-cv-174, 2012 WL 12879 (W.D. Okla. Jan. 4, 2012), in finding the allegations regarding the duty owed by the merchant to the issuing bank were insufficient, the court focused on the bank's failure to allege that the merchant had a "*special* responsibility" to the bank under Oklahoma law, which distinguishes it from Minnesota and its statutory law. *Id.* at *4; *see* Minn. Stat. § 325E.64.

Lastly, *CUMIS Insurance Society, Inc. v. Merrick Bank Corp.*, No. 07-cv-374, 2008 WL 4277877 (D. Ariz. Sept. 18, 2008), did not actually analyze whether the defendant owed the plaintiff a duty under the general negligence claim; instead the court focused only upon plaintiff's negligence misrepresentation claim. *Id.* at *11-12.

[6] Defendants argue that *Sovereign Bank* is not instructive because the Minnesota Supreme Court "has consistently stated that courts should be reluctant to impose new duties between businesses." (Defs.' Mem. at 12.) As set forth above, however, the *Erickson* and *Funchess* cases are inapplicable. *See* Minn. Stat. § 325E.64, subd. 3.

the kinds of damages alleged – stemming primarily from card replacement and charging off fraudulent transactions – are straightforward." *Id.* at *22-23 (emphasis added).[7]

The same is true here–Financial Institutional Plaintiffs are an identifiable class, and the damages are similar to those in *Heartland*, and Target owed a duty of care to them as foreseeable victims. *See id.*; *see also* Minn. Stat. § 325E.64, subd. 3.

2. Target is liable to Financial Institution Plaintiffs under the negligence *per se* or negligent misrepresentation/omission theories.

Target's assertion that Financial Institution Plaintiffs cannot plead negligence *per se*, negligent misrepresentation or negligent omission claims similarly falls flat. With respect to the negligence *per se* allegations, the Minnesota Plastic Card Security Act unequivocally provides that where there is a breach of the security system for a merchant (or their service provider) that has violated the Act, financial institutions have remedies against the merchant. *See id.* Target's only retort is that Plaintiffs assert "conclusory allegations," (Defs.' Mem. at 15), but this argument carries no weight as Plaintiffs have not yet even filed their Consolidated Complaint. Moreover, "[i]n Minnesota, violation of a statute which imposes a duty of care is negligence *per se* unless the statute specifically provides that the statute's violation is only prima facie evidence of negligence." *Ruhland v. Smith*, Nos. C7-91-668, C4-91-675, 1991 WL 257962, at *3 (Minn. Ct. App. Dec. 10,

[7] The district court's analysis of the duty owed to the financial institution plaintiffs was affirmed by the Fifth Circuit. *See Lone Star Nat'l Bank*, 729 F.3d at 426 ("Heartland may owe the Issuer Banks a duty of care and may be liable for their purely economic losses.").

1981). Target does not argue that the Minnesota Plastic Card Security Act limits its scope in such a manner.[8]

Similarly, Target argues that any negligent misrepresentation or omission claims are deficient because they do not allege that Target's representations caused Financial Institution Plaintiffs to "join[], remain[] in, or withdraw[] from the Visa [or] MasterCard networks," and therefore do not meet the heightened pleading requirement of Fed. R. Civ. P. 9(b). (Defs.' Mem. at 15.) To the extent Financial Institution Plaintiffs are even required to meet a fraud pleading standard, the Court will make that determination at the appropriate stage after the consolidated complaint is filed. Moreover, Target does not argue that reliance for negligent statements is only established by pleading that plaintiffs acted to "join[], remain[] in, or withdraw[] from the Visa [or] MasterCard networks." *See CUMIS Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.*, 2005 WL 6075375, at *4 (Mass. Super. Dec. 7, 2005) (denying motion to dismiss claims for negligent misrepresentation and stating that "[n]egligent misrepresentation claims are typically left to the jury").

3. Financial Institution Plaintiffs' contract-based allegations are valid.

Target similarly argues that Financial Institution Plaintiffs' breach of contract claims "are doomed to dismissal" because some courts in other data breach actions have dismissed certain contract-based allegations. (Defs.' Mem. at 16.) This assertion wrongly presupposes that Financial Institution Plaintiffs' allegations will mirror those

[8] Financial Institutional Plaintiffs reserve their right to assert claims for negligence *per se* under other statutes, including, *inter alia*, 15 U.S.C. § 1681 and 16 C.F.R. § 681.1, as well as pleading non-negligence claims under state consumer protection statutes and/or other laws and regulations.

asserted by plaintiffs in other cases. Again, Target argues for dismissal without the benefit of actually seeing the Consolidated Complaint's breach of contract count.

Moreover, noticeably absent from Target's analysis is *Sovereign Bank* in which the Third Circuit Court of Appeals reversed the district court's grant of summary judgment to acquirer bank Fifth Third on the breach of contract claim. In that case, credit card issuer Sovereign Bank brought an action against merchant BJ's Wholesale Club ("BJ's") and acquirer bank Fifth Third that processed credit card transactions, asserting claims for breach of contract relating to costs incurred by Sovereign Bank to issue new cards and reimburse cardholders for unauthorized charges to their accounts after BJ's computer system was hacked and cardholders' account numbers were stolen. *Sovereign Bank*, 395 F. Supp. 2d at 189-190. The district court granted summary judgment on defendants' breach of contract claim, which was reversed on appeal. *Sovereign Bank v. BJ's Wholesale Club, Inc.*, No. 05-cv-1150, 2006 WL 1722398, at *13 (M.D. Pa. June 16, 2006), *rev'd,* 533 F.3d 162, 173 (3d Cir. 2008). Financial Institution Plaintiffs will present a cognizable basis for a contractual claim. Additionally, *Sovereign Bank* underscores the importance of discovery in data-breach actions. Indeed, the Third Circuit relied upon deposition testimony and paper discovery reversing summary judgment. 533 F.3d at 173. This further refutes any argument by Target that discovery should be stayed in this case.

The above-referenced data breach cases, including *Heartland*, *TJX*, and *Sovereign Bank*, make it virtually certain that Financial Institution Plaintiffs' claims will proceed to discovery. A stay of discovery is patently unwarranted.

C. Target's challenges to Consumer Plaintiffs' standing and the merits of their claims are premature and wrong.

Likewise, Target's contention that Consumer Plaintiffs lack standing is for another day (Defs.' Mem. at 6-10); it will be addressed fully after Consumer Plaintiffs file their consolidated complaint (due August 25, 2014) and Target submits its motion to dismiss (due October 1, 2014). But if the Court were to consider these arguments at this stage, even the brief analysis below demonstrates that Target is wrong under the facts and well-settled jurisprudence.

Target's premature challenge to Consumer Plaintiffs' standing based on its assertion of lack of harm caused by the data breach is startling. It ignores the facts. The credit and debit card information of 40 million members of the putative class in the possession of Target was compromised and the personal information, including email and mailing addresses and phone numbers, of up to 70 million members of the putative class was exposed. Yet Target claims that no consumer has standing to challenge Target's conduct. Target's position defies common sense and the already known, egregious consequences of the data breach. The Senate Committee Report states:

> [t]hieves were able to sell information from these cards via online black market forums known as "card shops." Those purchasing the information can then create and use counterfeit cards with the track data and PIN numbers stolen from credit and debit card magnetic stripes. Fraudsters often use these cards to purchase high-dollar items and fence them for cash, and if PIN numbers are available, ***a thief can extract a victim's money directly from an ATM.***

Senate Committee Report at 1-2 (emphasis added). *Bloomberg Businessweek* reported:

> For Minnetonka, about 12 miles from Target's headquarters with a population of 51,000, there are 7,000 cards for sale. For another

> Minneapolis suburb, Plymouth, population 73,000, there are 5,335 cards available. Fayetteville, Ark.: 3,685. Torrington, Conn.: 5,115. The [stolen] cards run from $6 a piece for a prepaid gift card to almost $200 for an American Express Platinum, and Rescator accepts payments in Bitcoin and Western Union (WU). The return period – just in case some of the cards don't work – is six hours . . . Long before six hours elapse, thieves can have the stash of stolen numbers printed on counterfeit cards and charge up a storm of purchases at stores or online, often in the form of gift cards that are easily transformed into cash.

Bloomberg Businessweek, Mar. 13, 2014, http://www.businessweek.com/articles/2014-03-13/target-missed- alarms-in-epic-hack-of-credit-card-data#4.

1. Consumer Plaintiffs satisfy traditional standing requirements.

The long settled constitutional Article III standing requirements are injury, causal relationship and redressability. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992); *Steger v. Franco, Inc.*, 228 F.3d 889, 892 (8th Cir. 2000) (stating that "[t]o show Article III standing, a plaintiff has the burden of proving: (1) that he or she suffered an 'injury-in-fact,' (2) a causal relationship between the injury and the challenge conduct, and (3) that the injury likely will be redressed by a favorable decision") (citing *Lujan*). Consumer Plaintiffs have alleged in numerous actions and will allege in their consolidated complaint, that Target's unlawful conduct injured Plaintiffs and all members of the proposed nationwide class. The injury-in-fact takes several forms, including unauthorized charges on their debit and credit card accounts, theft of their personal and financial information, costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts, costs associated with inability to obtain money from their accounts and the substantial, certainly impending injury flowing from

potential fraud and identity theft posed by the exposure of their credit card and personal identifying information that has been placed in the hands of thieves and misused via sale of consumers' information on the black market.[9] Consumer Plaintiffs assert that the harm they suffered is the direct result of Target's unlawful conduct.[10] The injury suffered by Consumer Plaintiffs is redressable. The availability of a judgment providing for redress for the injuries suffered by Consumer Plaintiffs and the proposed consumer class and appropriate injunctive relief to require Target to maintain adequate security measures to protect the personal and financial information in its possession demonstrates that the redressability prong of constitutional standing is easily satisfied.

Even in cases **not** involving the straightforward injuries directly flowing from the Target data breach – economic losses, including unauthorized charges to various Consumer Plaintiffs' accounts and the sale of consumers' personal information on the black market exposing all consumers to the clearly imminent harm of fraud and misuse of their credit and debit card accounts – courts have found that plaintiffs in data breach cases have standing. That is, in several cases in which a theft of data subjects plaintiffs to an increased risk of future identity theft or misuse, courts have found Article III standing even though, unlike in this case, no actual misuse has yet occurred. For example, the Court of Appeals for the Seventh Circuit has held that the threat of future harm is

---

[9] Using but one of the many consumer case complaints as an illustration, *see Mancias v. Target Corp.* No. 0:14-cv-01090-PAM-JJK (Filed Jan. 14, 2014), Class Action Compl. ¶¶ 5, 71, 86, 96 and 115.

[10] *See, e.g., Mancias v. Target Corp.*, Compl. ¶¶ 48-53, 70-71, 96, 106, 115-16.

sufficient to confer standing. *See Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (holding that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced absent the defendant's actions."). Similarly, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140 (9th Cir. 2010), a laptop containing the names, addresses and social security numbers of approximately 97,000 employees was stolen from Starbucks. Plaintiffs did not allege any misuse, but the Ninth Circuit nevertheless held that plaintiffs, "whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III." *Id.*

Supreme Court precedent and federal court decisions recognizing standing based on the invasion of legal rights further support Consumer Plaintiffs' standing. In *Havens Realty Corp. v. Coleman*, 455 U.S. 363 (1982), individuals and an organization, including "testers" hired to determine whether defendant practiced racial steering in renting defendants' apartments, sued under the Fair Housing Act. *Id.* at 363. "As we previously recognized, '[t]he actual or threatened injury required by Art. III may exist solely by virtue of "statutes creating legal rights, the invasion of which creates standing . . . ."'" *Id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975) (additional citations omitted)). The Court concluded that since the FHA "establishes an enforceable right to truthful information concerning the availability of housing," a tester subject to a misrepresentation made unlawful under the statute "has suffered injury in precisely the form the statute was intended to guard against, and therefore has standing to maintain a claim for damages . . . ." *Id.* at 373-74; *see also Katz v. Pershing, LLC*, 672 F.3d 64, 72

(1st Cir. 2012) (noting that "[t]he invasion of a common-law right (including a right conferred by contract) can constitute an injury sufficient to create standing") (citing *Ala. Power Co. v. Ickes*, 302 U.S. 464, 469 (1938)). Thus, Target's conduct giving rise to violations of Consumer Plaintiffs' rights conferred by statute (such as consumer protection statutes or state data breach notice statutes) or protected by such common law causes of action as negligence or breach of implied contract, further support Consumer Plaintiffs' standing.

2. The Supreme Court's *Clapper v. Amnesty International USA* decision supports Consumer Plaintiffs' standing.

In prematurely challenging Consumer Plaintiffs' standing, Target relies upon *Clapper v. Amnesty International USA*, __ U.S. __, 133 S. Ct. 1138 (2013). *Clapper* supports Consumer Plaintiffs' standing. The Supreme Court reaffirmed the established Article III standing requirements of "actual or imminent" injury "fairly traceable to the challenged action" and "redressable by a favorable ruling." *Clapper*, 133 S. Ct. at 1147 (citations omitted). The Court stated that "we have repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact.'" *Id.* Consumer Plaintiffs have suffered both actual and imminent injury in fact. The threat of further harm through the increased risk of fraud and misuse is unquestionably "certainly impending." The cyber thieves are criminals. They breached Target's computer systems for the express purpose of accessing customers' valuable credit and debit card and personal information to misuse it. That misuse has occurred. Thieves have sold consumers' information on the credit card black market. It is difficult to imagine facts more clearly demonstrative of

actual and certainly impending further misuse of consumers' personal identifying information.

Under similar facts, the First Circuit found that customers whose electronic payment data was allegedly stolen by third-party hackers had shown a cognizable injury as required for their negligence and breach of contract claims under Maine law against the grocery store whose computer system was breached. *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 154 (1st Cir. 2011). The hackers stole up to 4.2 million credit and debit card numbers, expiration dates and security codes but not customer names. *Id.* The grocery store acknowledged receiving reports of approximately 1,800 cases of fraud resulting from the theft. *Id.* The First Circuit allowed the customers to pursue mitigation cost damages, reasoning:

> This case involves a large-scale criminal operation conducted over three months and the deliberate taking of credit and debit card information by sophisticated thieves intending to use the information to their financial advantage. Unlike the cases cited by Hannaford, this case does not involve inadvertently misplaced or lost data which has not been accessed or misused by third parties. Here, there was actual misuse, and it was apparently global in reach. The thieves appeared to have expertise in accomplishing their theft, and to be sophisticated in how to take advantage of the stolen numbers. The data was used to run up thousands of improper charges across the globe to the customers' accounts. The card owners were not merely exposed to a hypothetical risk, but to a real risk of misuse.
>
> Further, there is no suggestion there was any way to sort through to predict whose accounts would be used to ring up improper charges. By the time Hannaford acknowledged the breach, over 1,800 fraudulent charges had been identified and the plaintiffs could reasonably expect that many more fraudulent charges would follow. Hannaford did not notify its customers of exactly what data, or whose data, was stolen. It reasonably appeared that all Hannaford customers to have used credit or debit cards during the class period were at risk of unauthorized charges.

659 F.3d at 164; *see also F.T.C. v. Wyndham Worldwide Corp.*, No. 13-1887 (ES), 2014 WL 1349019, at *16-17 (D.N.J. April 7, 2014) (denying motion to dismiss FTC claims that defendant engaged in unfair and deceptive practices in failing to safeguard customers' personal information, rejecting defendants' argument consumers did not suffer injury because federal law caps consumer law liability for certain card purchases, and crediting FTC's allegations that consumers suffered substantial financial injury, including unreimbursed fraudulent charges, increased costs, lost access to funds or credit and time and money resolving fraudulent charges and mitigating subsequent harm).

The Supreme Court's *application* of the established standing criteria in *Clapper*, of course, was to facts that could not be more different. In *Clapper*, plaintiffs, including attorneys and human rights and media organizations, sought a declaratory judgment that provisions of a federal statute allowing surveillance of individuals who were not "United States persons" and were located outside the United States was unconstitutional. 133 S. Ct. at 1142. The Supreme Court held that plaintiffs lacked Article III standing because they did not demonstrate that the claimed threatened injury was "certainly impending" and therefore had not established injury-in-fact. *Id.* at 1143.

Clapper is readily distinguishable. *Clapper* was concerned exclusively about whether a future event would ever happen. The Supreme Court found that "respondents fail to offer any evidence that their communications have been monitored." *Id.* at 1148. This case, by contrast, does not involve speculation about the occurrence of some future event. The extraordinarily sweeping Target data breach has occurred. Its consequences, including economic losses incurred by Consumer Plaintiffs and the not speculative but

very real, concrete, imminent threat arising from the sale of Consumer Plaintiffs' and class members' account and personal information on the fake credit card black market have already occurred. This is not a case about speculating what the future holds; it is about seeking accountability for Target's conduct directly resulting in injury-in-fact suffered by every Consumer Plaintiff whose credit or debit card and/or personal identifying information has been compromised and is available for sale and being sold by criminals. Moreover, this same information remains in the possession of Target, and Consumer Plaintiffs have both an interest and a right to ensure that this information is protected from further loss.

In *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, No. 11-md-2258 (AJB) (MDD), 2014 WL 223677 (S.D. Cal. Jan. 21, 2014), Sony made the same argument Target makes here, urging that *Clapper* required dismissal on grounds that plaintiffs lacked Article III standing. *Id.* at *7. The court was unpersuaded, stating that "the Supreme Court's decision in *Clapper* did not set forth a new Article III framework" but rather "simply reiterated an already well-established framework for assessing whether a plaintiff had sufficiently alleged an 'injury-in-fact' for purposes of establishing Article III standing." *Id.* at *8. The *Sony* court found that "Plaintiffs' allegation that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion sufficient to establish Article III standing at this stage in the proceedings." *Id.* at *9.

3. Target's cited cases are inapposite or readily distinguishable.

Target cites a number of cases in which courts have found plaintiffs lacked standing in data breach cases. (Defs.' Mem. at 6-8.) None should give this Court pause. The cited cases are far removed from the facts of this case and serve only to underscore the Court's traditional role of considering the facts actually before it. *See Baur v. Venneman*, 352 F.3d 625, 637 (2d Cir. 2003) (observing that "[l]ike all other aspects of standing, the injury-in-fact analysis is highly case-specific"). Target's cited cases fall on the far side of a line of demarcation between cases involving facts of actual misuse, including unauthorized charges,[11] and certainly impending further harm from further misuse of breached data (here, a massive criminal theft of private data inflicting actual, and clearly imminent additional injury from the dissemination, misuse and sale of consumers' breached information on an Internet black market) and cases involving no

[11] Target asserts that "none of the named plaintiffs in the underlying complaints alleges that she has incurred present, out-of-pocket costs as a result of the Intrustion." (Defs.' Mem. at 8.) This assertion is simply incorrect. In the complaints already filed, numerous consumers do, in fact, allege incurring unauthorized charges to their accounts. To use but one example, *see Reynoso v. Target Corp.*, No. 0:14-cv-00347 (D. Minn. filed Feb. 7, 2014), Class Action Complaint. Martha Reynoso, a resident of Chicago, alleges that she uses a debit card issued through the State of Illinois for child support for her son. She used her debit card to make purchases at Target stores between Nov. 27 and Dec. 15, 2013. On December 28, 2013, virtually all of her money was taken from her account in a series of international ATM transactions occurring over just a few minutes. The cash withdrawals, including international transaction fees, depleted her account balance from $3,643.53 to $5.86. These large withdrawals outside of the U.S. were inconsistent with Ms. Reynoso's pattern of using her debit card for purchases made within Illinois and for far smaller amounts than the unauthorized transactions. *Reynoso* Compl. ¶¶ 13-14.

misuse but only speculative future harm.[12] The facts of those cases are far different from the actual theft and misuse of data following the massive Target data security breach that has resulted in classic injury in fact to Consumer Plaintiffs and all members of the proposed consumer class.

4. Consumer Plaintiffs' claims are valid and not subject to dismissal at the motion to dismiss stage.

Now is not the time to engage in a Rule 12(b)(6) analysis. Target assumes that its not-yet-filed motion to dismiss will succeed in eliminating or narrowing Consumer Plaintiffs' claims in their not-yet-filed consolidated complaint. Target's assumption is

[12] *See, e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) (denying standing where "no evidence suggests that the data has been – or will ever be – misused"); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307, at **2,7-8 (S.D.N.Y. June 25, 2010) (no evidence the information had been accessed or used inappropriately); *Allison v. Aetna, Inc.*, No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010) (court noted plaintiff's allegation that his personal information was even accessed was conjectural and plaintiff did not allege that anyone else had obtained the breached information); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052 (E.D. Mo. 2009) (no publication of any wrongfully obtained information nor fraudulent or otherwise harmful use of the information and "plaintiff does not claim that his personal information has in fact been stolen"); *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 794, 796 (M.D. La. 2007) (defendant "had no indication that any unauthorized individual had used personal information contained in the data" and plaintiff did not allege misuse of his private information); *Bell v. Acxiom Corp.*, No. 06-cv-00485, 2006 WL 2850042, at *1, *2 (E.D. Ark. Oct. 3, 2006) (the plaintiff had not pled "that she has received a single marketing mailer" and "does not know whether her name and information were contained within the databases stolen"); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (no evidence that plaintiff's information was obtained and used by an unauthorized person for an unlawful purpose and plaintiff did not allege evidence that a third-party intends to make unauthorized use of her financial information); *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 704, 711 (D.C. 2009) (no evidence that home burglary was for the specific purpose of obtaining the information on stolen laptop, no evidence that "any exposure of Plaintiff's personal information" had occurred, and no allegation that the data "were disclosed to and viewed by someone unauthorized to do so").

untethered to the facts or law. The same argument has been rejected as a reason for staying discovery, because it "require[s] the court to make a preliminary finding of the likelihood of success on the motion to dismiss . . . circumvent[ing] the procedures for resolution of such a motion." *Gray v. First Winthrop Corp.*, 133 F.R.D. 39, 40 (N.D. Cal. 1990); *Gerald Chamales Corp. v. Oki Data Americas, Inc.*, 247 F.R.D. 453, 454 (D.N.J. 2007) (rejecting argument that plaintiff's claim lacks merit as grounds for discovery stay pending motion to dismiss). Target points to instances in which courts have narrowed or dismissed at the pleading stage various claims in other data breach cases. (Defs.' Mem. at 8-10.) Each case is different, presenting its own facts. Not once in Target's discussion of what courts under different facts have done in other data breach cases does Target discuss the specific facts of the case now before this Court.

To the extent that the Court nevertheless desires to take a "peek" at the merits of Target's anticipated motion to dismiss, *see TE Connectivity Networks, Inc.*, 2013 WL 4487505, at *2, Consumer Plaintiffs submit that the allegations in the plaintiffs' complaints already filed amply set forth valid claims for relief against Target on various grounds. Plaintiffs are fully confident of the claims they will set forth in their upcoming consolidated complaints. For example, and without limitation, Consumer Plaintiffs will assert that Target's failure to reasonably secure and protect its customers debit and credit card account and personally identifying information constitutes negligence,[13] breach of

[13]*See, e.g., Mancias v. Target Corp.*, No. 0:14-cv-01090-PAM/JJK (Filed Jan. 14, 2014), Class Action Complaint alleging facts showing that the vulnerability of corporate point-of-sale systems was made known to Target years before the data breach occurred

implied contract,[14] and violations of state consumer laws[15] and that its failure to provide timely notice of the data breach violates various state data breach notice statutes.[16] At the

---

(¶¶ 22-30), detailing the data breach and Target's failure to promptly and accurately notify the public (¶¶ 31-47), setting out the harm caused by the data breach to plaintiffs and class members (¶¶ 48-53) and setting forth the elements of and factually supported claims for relief, including negligence (Count I).

[14] For example, in *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011), in affirming that plaintiffs' implied contract claim could proceed, the First Circuit reasoned:

> The district court correctly concluded that a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would not use the credit card data for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information. When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect – and certainly does not intend – the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.

[15] For example, in *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, the district court denied defendant's motion to dismiss plaintiffs' claims based on various state consumer protection statutes, including on an omission theory. *See, e.g., Sony*, 2014 WL 223677, at *34 (denying motion to dismiss plaintiffs California consumer law omissions claims). State consumer laws generally cover omissions of material facts. *See, e.g., State of Minn. v. Fleet Mortg. Corp.*, 158 F. Supp. 2d 962, 967 (D. Minn. 2001); *Graphic Commc'ns Local 1B Health & Welfare Fund "A" v. CVS Caremark Corp.*, No. A12-1555, 2014 WL 2965400, at *10 (Minn. July 2, 2014). Under Minnesota law, a fact is material "if it would naturally affect the conduct of the party addressed." *Yost v. Millhouse*, 373 N.W.2d 826, 830 (Minn. Ct. App. 1985). Target's failure to disclose that it did not have reasonable safeguards and data security in place is clearly material information that would have influenced consumers' purchasing decisions.

[16] Forty seven states have statutes requiring businesses to provide timely notice of any breach of the security of their computerized data systems. *See, e.g.*, The California Data Breach Act, Cal. Civ. Code § 1798.80, *et seq.* At the appropriate time (in their opposition to Target's motion to dismiss), Consumer Plaintiffs will provide the Court

appropriate time, Plaintiffs will fully brief any motion to dismiss filed by Target. On the issue now before the Court, Target has simply not met its burden under Rule 26(c). A stay of discovery is not warranted.

D. Target has not met its burden to stay discovery.

Setting aside Target's arguments in support of a stay based on its anticipated filing of motions to dismiss, which as explained *supra* are legally deficient to warrant a discovery stay, *see TE Connectivity Networks*, 2013 WL 4487505, at *2, the only basis for Target's claim of "burden" appears to be that Plaintiffs have ***proposed*** written discovery and depositions in excess of the standards set forth in the Federal Rules.[17] *See Lubrication Techs., Inc. v. Lee's Oil Servs., LLC*, 2012 WL 1633259, at *13 (D. Minn. Apr. 10, 2012) (stating that "[b]road allegations of harm, unsubstantiated by

---

with complete briefing on Target's violations of applicable state data breach notice statutes. Target contends in a footnote that "[n]o court could fairly conclude that the short time period between Target's discovery of the breach and its notification was unreasonable." (Defs.' Mem. at 9-10 n.9.) Plaintiffs have alleged facts indicating that Target breached state data breach notice statutes. *See, e.g., Mancias v. Target Corp.* Compl. ¶¶ 31-47 (detailing the data breach and Target's failure to promptly and accurately notify customers) and Count V (alleging violations of the California Data Breach Act, Cal. Civ. Code § 1798.80, *et seq.*, requiring that "disclosure shall be made in the most expedient time possible and without unreasonably delay"). The parties' quite different positions on compliance by Target with state data breach notice laws obviously raise fact questions to be resolved on the merits following discovery.

[17] In Consumer Plaintiffs' and Target's Joint Rule 26(f) Report, Consumer Plaintiffs *and Target* indicated that *the parties* anticipate that "this complex litigation will require deposition and interrogatory discovery that exceeds the limits" of Fed. R. Civ. P. 30(a)(2)(A)(i) and 33(a)(1) and that if they are unable to agree, "the party seeking such discovery may ask the Court for leave to exceed the Federal Rules' limitations." Any actual, substantiated claim of burden can be raised at that time by Target or Plaintiffs, and if necessary, addressed by the Court.

specific examples or articulated reasoning do not support a good cause showing"); *see Baer*, slip op. at 2 (holding "[t]hose [Federal] Rules [of Civil Procedure], and particularly Rule 26(c), provide specific reasons for an order that discovery be suspended"). Given the complexity of the instant action (one of the largest data breaches in the history of the United States), discovery in excess of Rules 30(a)(2)(A) and 33(a)(1) will be required, but all of this discovery will not be conducted prior to a ruling on the impending motion to dismiss and Target has the ability to seek protective orders when it believes a specific request is unjustified under the Federal Rules.

Moreover, staying discovery would severely prejudice plaintiffs considering that motion to dismiss briefing will not conclude until October 22, 2014 (for Financial Institution Plaintiffs) and November 20, 2014 (for Consumer Plaintiffs) and that the class certification expert reports are due on April 1, 2015 and discovery cuts off within a year. (ECF Nos. 93, 94.) Target's generic claim that discovery will be too burdensome and should be stayed rings hollow.[18] *See Galaria v. Nationwide Mutual Ins. Co.*, 2013 WL

[18] Target's cited authorities are distinguishable. For example, in *Riehm v. Engelking*, No. 06-293 (JRT/RLE), 2006 WL 2085404, *2 (D. Minn. July 25, 2006), the court entered a stay where defendants had raised defenses of qualified and official immunity. No such defense is asserted by Target. Defendant's reliance on *Chavous v. Dist. of Columbia Financial Responsibility and Management Assistance Authority*, 201 F.R.D. 1 (D.D.C. 2001) is similarly unavailing. Although not mentioned by Target, the court in *Chavous* noted that "a stay of discovery pending determination of a motion to dismiss 'is ***rarely appropriate*** when the pending motion will not dispose of the entire case.'" 201 F.R.D. at 3 (citation omitted; emphasis added). In *Chavous*, the parties agreed that the granting of either the plaintiff's motion for summary judgment or the defendant's motion to dismiss would be dispositive of the entire case. *Id.* No such agreement exists here. Target also cites *Marrese v. American Academy of Orthopedic Surgeons*, 706 F.2d 1488 (7th Cir. 1983), an antitrust case in which Judge Posner

6578730, at *3 (S.D. Ohio Dec. 16, 2013) (denying a motion to stay in a putative class action pending a motion to dismiss where defendant failed to identify any specific discovery request that was unduly burdensome); *Solidfx, LLC v. Jeppesen Sanderson, Inc.*, 2011 WL 4018207, at *3 (D. Colo. Sept. 8, 2011) (rejecting a motion to stay discovery of antitrust claims and noting that the fact that the antitrust claims are complex is not reason enough to stay discovery and that the defendant failed to point to any particular discovery which would be burdensome); *New England Carpenters Health and Welfare Fund v. Abbott Labs.*, 2013 WL 690613, at *3 (N.D. Ill. Feb. 20, 2013) (denying a motion to stay discovery pending a motion to dismiss in a putative class action where defendants generically argue that class and merits discovery will be costly).[19]

For example, Plaintiffs have requested that Target produce documents that Target received from and submitted to any federal or state agencies investigating the data security breach (for example, the Department of Justice, the Federal Trade Commission,

---

reasoned that the district court should not have ordered discovery of defendant's membership files before plaintiff first engaged in discovery on the issue of anticompetitive effects of defendant's conduct. *Id.* at 1497. The case is inapposite.

[19] Target's reliance on *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), is misplaced. *Twombly* addressed pleading standards. Nothing in *Twombly* or *Iqbal* prevents discovery or directs district courts to stay discovery while motions to dismiss are pending. Courts have rejected any such misreading of *Twombly*. *See, e.g., In re Graphics Processing Units Antitrust Litig.*, No. 06-CV-07417, 2007 WL 2127577, at *4 (N.D. Cal. July 24, 2007) (reasoning that *Twombly* "did not use pleading standards to find a reason to foreclose all discovery"); *In re Flash Memory Antitrust Litig.*, No. 07-CV-0086, 2008 WL 62278, at *3 (N.D. Cal. Jan. 4, 2008) (noting that *Twombly* did not hold that discovery should be stayed until after a complaint survives a Rule 12(b)(6) challenge and that "[s]uch a reading of that opinion is overbroad and unpersuasive").

U.S. Secret Service, the FBI and State Attorneys General).[20] The requested materials are relevant under Rule 26. They are also easily produced without undue burden, since the documents have already been gathered, presumably reviewed by counsel and produced to investigating federal and state agencies. The production of these initial documents will of course be safeguarded and governed by the Court's Protective Order. (ECF No. 92.) Courts routinely allow the production of a limited subset of documents prior to resolution of a motion to dismiss. *See, e.g.*, *In re Lipitor Antitrust Litig.*, MDL No. 2332, No. 12-cv-2389, Order (D.N.J. Oct. 19, 2012) (ECF No. 197) (denying motion to stay discovery pending resolution of motions to dismiss and noting the reasonableness of plaintiffs' limited initial discovery requests focused on documents previously produced in other relevant litigation or submitted to the Patent and Trademark Office and the FDA) (Bores Decl. Ex. C); *In re Dairy Farmers of Am. Inc. Cheese Antitrust Litig.*, No. 09-cv-03690, Order (N.D. Ill. Mar. 4, 2010) (ECF No. 75) (refusing to stay discovery with regard to materials previously produced to the CFTC) (Bores Decl. Ex. D). Prompt production of these initial easily produced documents will expedite discovery and allow Plaintiffs to focus and facilitate subsequent discovery.

In resisting production of materials it has already provided to investigating federal or state agencies, Target cites a case stating that "the compelled act of turning records over to the government . . . does not mean that everyone else has an equal right to

[20] Plaintiffs made the request in correspondence dated June 30, 2014 from Karl L. Cambronne to all Defendants' counsel and in an email dated July 1, 2014, from Vincent J. Esades to Target's counsel. Target responded in correspondence from Wendy J. Wildung, declining Plaintiffs' request.

rummage through the same records." (Defs.' Mem. at 24 (citing *In re Graphics Processing Units Antitrust Litig.*, No. C 06-07417, 2007 WL 2127577, at *5 (N.D. Cal. July 24, 2007).)[21] But Plaintiffs are not "everyone else" with an interest in "rummaging" through Target's records. They are Target's customers and their financial institutions. They seek access to documents Target has already produced to investigating agencies concerning a massive data breach – a breach that affected up to 110 million Target customers and thousands of financial institutions. Plaintiffs have a right to the information sought. It is relevant and readily producible. It should be produced now. To be clear, Plaintiffs are *not* suggesting limiting discovery prior to the Court's motion to dismiss ruling exclusively to materials Target has already produced to investigating agencies. Rather, Plaintiffs highlight their request for those materials as an illustration of why Target has not met its burden of demonstrating undue burden and to underscore the appropriateness of and Plaintiffs' need for the immediate production of those materials.

IV. CONCLUSION

For these reasons, Target's motion to stay of discovery should be denied in its entirety. Target has not heeded the Court's previous instruction to persuade it that Target could meet the high standard needed to stay discovery. *See In re Target Corp. Customer*

[21] In that private civil antitrust case involving a pending federal criminal antitrust investigation, the court stayed discovery pending resolution of defendant's motion to dismiss. 2007 WL 212577, at *1. In doing so, the court referenced an unpublished decision within the same district denying a stay request under similar circumstances and ordering production of materials previously produced by the defendant to DOJ's Antitrust Division. *Id.* at *5. *See In Re Static Random Access Memory (SRAM) Antitrust Litig.*, No. 07-md-01819 CW, Suppl. Case Mgmt. Order No. 1 (N.D. Cal. June 21, 2007) (Bores Decl. Ex. E).

Data Sec. Breach Litig., No. 14-md-2522, May 14, 2014 Status Conference Tr. at 11.

Plaintiffs believe there is no need for a hearing on Target's motion.

Dated: July 18, 2014

CHESTNUT CAMBRONNE PA

By: s/Karl L. Cambronne
Karl L. Cambronne (#14321)
kcambronne@chestnutcambronne.com
Jeffrey D. Bores (#227699)
jbores@chestnutcambronne.com
Bryan L. Bleichner (#0326689)
bbleichner@chestnutcambronne.com
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
(612) 339-7300
Fax (612) 336-2940

Coordinating Lead Counsel

ZIMMERMAN REED, PLLP

By: s/Charles S. Zimmerman
Charles S. Zimmerman
charles.zimmerman@zimmreed.com
J. Gordon Rudd, Jr. (#222082)
gordon.rudd@zimmreed
Brian C. Gudmundson (#336695)
brian.gudmundson@zimmreed.com
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400

Lead Counsel Financial Institution Cases

HEINS MILLS & OLSON, P.L.C.

By: s/Vincent J. Esades
Vincent J. Esades (#249361)
vesades@heinsmills.com
David Woodward (#018844X)
dwoodward@heinsmills.com
310 Clifton Avenue
Minneapolis, MN 55403
(612) 338-4605
Fax: (612) 338-4692

Lead Counsel Consumer Cases